

SEALED

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FILED

AUG - 9 2018

**Holding a Criminal Term
Grand Jury Sworn in May 3, 2018**

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

UNITED STATES OF AMERICA

v.

JONG WOO SON,

Defendant.

Criminal No. _____

Magistrate No. **1:18-0019 (GMH)**

Violations:

**18 U.S.C. §§ 2251(d) and (e)
(Conspiracy to Advertise Child
Pornography)**

**18 U.S.C. § 2251(d)
(Advertising of Child Pornography)**

**18 U.S.C. § 2260(b)
(Production of Sexually Explicit
Depictions of a Minor for Importation
into the United States)**

**18 U.S.C. §§ 2252(a)(2) and (b)(1)
(Conspiracy to Distribute Child
Pornography)**

**18 U.S.C. § 2252(a)(2)
(Distribution of Child Pornography)**

**18 U.S.C. § 1956(a)(2)(A)
(Laundering of Monetary Instruments)**

**FORFEITURE:
21 U.S.C. § 853; 18 U.S.C. § 982;
18 U.S.C. §§ 981 and 2253**

UNDER SEAL

Case: 1:18-cr-00243
Assigned To : Judge McFadden, Trevor N.
Assign. Date : 8/9/2018
Description: INDICTMENT (B)

INDICTMENT

The Grand Jury charges that:

At times material to this Indictment:

DEFINITION OF TERMS

The Tor Network

1. Tor was a computer network which anonymized Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ("IP") address of the user.

2. An "IP address" was a unique numeric address (used by computers on the internet) that is assigned to properly direct internet traffic. A publically visible IP address could allow for the identification of the user and his/her location.

3. To access the Tor network, a user had to install freely available Tor software, which relayed only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address. There was no practical method to trace a user's actual IP address back through those Tor relay computers.

4. The Tor network made it possible for a user to operate a special type of website, called "hidden services," which used a web address that is comprised of a series of 16 algorithm-generated characters (such as "asdlk8fs9dfiku7f") followed by the suffix ".onion." Websites, including hidden services, had system administrator(s) (also called the "admin(s)") who were responsible for overseeing and operating these websites.

Bitcoin

5. Bitcoin (“BTC”) was one type of virtual currency that was circulated over the Internet.

6. BTC was not issued by any government, bank, or company, but rather was controlled through computer software.

7. Generally, BTC was sent and received using a BTC “address,” which was like a bank account number and was represented by a case-sensitive string of numbers and letters. Each BTC address was controlled through the use of a unique private key, a cryptographic equivalent of a password. Users could operate multiple BTC addresses at any given time, with the possibility of using a unique BTC address for every transaction.

8. BTC fluctuated in value. As of March 5, 2018, one BTC was worth approximately \$11,573.00.

9. A typical user purchased BTC from a BTC virtual-currency exchange, which was a business that allowed customers to trade virtual currencies for conventional money (*e.g.*, U.S. dollars, euros, etc.).

10. Little to no personally identifiable information about the sender or recipient was transmitted in a BTC transaction itself. However, virtual currency exchanges were required by U.S. law to collect identifying information of their customers and verify their clients’ identities.

11. To send BTC to another address, the sender transmitted a transaction announcement, cryptographically signed with the sender’s private key, across the BTC network.

12. Once the sender’s transaction announcement was verified, the transaction was added to the blockchain.

13. The blockchain was a decentralized, public ledger that logged every BTC transaction.

14. In some instances, blockchain analysis could reveal whether multiple BTC addresses were controlled by the same individual or entity.

15. For example, analyzing the data underlying BTC transactions allowed for the creation of large databases that grouped BTC transactions into “clusters.” This analysis allowed for the identification of BTC addresses that were involved in transacting with the same addresses.

WELCOME TO VIDEO WEBSITE

The Welcome To Video Website

16. The defendant was the administrator of Welcome To Video, a Tor network-based child-pornography website, which began operating at least in or about June 2015.

17. Welcome To Video hosted and distributed image and video files depicting child pornography. The upload page on Welcome To Video stated: “Do not upload adult porn.”

18. On or about February 8, 2018, Welcome To Video indicated on its download page details that its users had downloaded files from Welcome To Video more than a million times.

19. On or about March 5, 2018, the Welcome To Video server had over 200,000 unique video files, which totaled approximately eight terabytes of data.

20. Each video available for download had a title, a description (if included by the uploader), “tags” with further descriptions of the video, and a preview thumbnail image that contained approximately sixteen unique still images from the video.

21. The video search page of Welcome To Video listed keyword search terms and the number of videos associated with each keyword. On or about February 8, 2018, some of the top

keyword search terms and the associated approximate videos included “PTHC,” “PEDO,” “%2yo,” “%4yo,” and “incest.”

- a. “PTHC” is an abbreviation for “preteen hardcore.”
- b. “Pedo” is an abbreviation for “pedophile.”
- c. “%2yo” is an abbreviation for “2 year old.”
- d. “%4yo” is an abbreviation for “4 year old.”

22. Welcome To Video contained instructions on how these videos could be downloaded by customers.

23. Any customer could create a free account on Welcome To Video by creating a username and password. After the customer had an account, the customer could browse picture previews of videos depicting child pornography that were available for download.

24. To download videos from Welcome To Video, the customer redeemed “points.” A customer could obtain points by: (1) uploading videos depicting child pornography; (2) referring new customers to the website; (3) paying 0.03 BTC (approximately \$352.59 as of March 5, 2018) for a “VIP” account, which lasted for six months and purportedly allowed unlimited downloads; and/or (4) paying for points incrementally (*i.e.*, 0.02 bitcoin for 230 points).

25. Co-conspirators who uploaded videos to Welcome To Video would earn “points” each time someone downloaded that video from Welcome To Video.

26. Points were not transferable to any other website or application. Once a customer sent BTC to Welcome To Video, the BTC could not be refunded or redirected. The points obtained by the payment of BTC could only be used for downloading videos.

27. Once a video was uploaded to Welcome To Video, the uploader was not able to

delete the video. However, the administrator retained access to these videos.

28. Welcome To Video directed customers to particular BTC exchangers to make payments to it, including an exchanger in the United States.

29. Welcome To Video established unique BTC addresses to receive payments from each different Welcome To Video customer account. In total, Welcome To Video had set up over 1.3 million BTC addresses.

30. Law enforcement clustered thousands of unique BTC addresses together as associated with Welcome To Video. This cluster included an undercover agent's BTC address which Welcome To Video assigned to the undercover agent when the undercover agent created an account on Welcome To Video.

31. From in or about June 2015 to on or about March 8, 2018, Welcome To Video received at least 420 BTC through at least 7,300 transactions worth over \$370,000.00 at the time of the respective transactions.

32. Customers from numerous countries, including the United States, Great Britain, and South Korea, sent BTC to Welcome To Video.

33. An MD5 hash is the result of applying a complex algorithm to the ones and zeros that make up a computer file. For example, two identical picture files will have the same hash value. If you took one of the pictures and changed a single pixel, you would be changing the ones and zeros that make that computer file. Therefore, it would be a completely different hash value when the algorithm is applied. The hash value would not tell you how the file changed, only that it has changed because it resulted in a different hash value.

34. Welcome To Video would not allow a customer to upload a video that had been

previously uploaded to the site. Welcome To Video enforced this by providing an MD5 hash-value check for customers to compare their video(s) to other videos previously uploaded.

35. On multiple occasions, an agent acting in an undercover capacity paid BTC to Welcome To Video and downloaded child pornography video files from it while in Washington, D.C.

36. These downloaded child pornography video files included pre-pubescent children, infants and toddlers engaged in sexually explicit conduct.

37. Video files downloaded from Welcome To Video included the following:

- a. File name “[pthc] 10y Tara Blowjob + Anal Riding Fuck (05min).avi” with the video tag description “Tara Riding Fuck” depicted a child, approximately ten years old, and an adult male inserting his penis into the child’s mouth and anus. Welcome To Video customers downloaded this video 957 times;
- b. File name “2 (2).avi” with the video tag description “Pedo Preteen Amateur Underage” depicted a female child approximately three years old. The child is nude and bound with her legs spread apart so that her genitalia is visible. An adult male urinates on her. Welcome To Video customers downloaded this video 219 times;
- c. File name “Rape Toddler Girl.mpg” with the video tag description “rape toddler” depicted a female toddler, approximately two or three years old. An adult male inserted his penis inside of the anus of the female toddler. Welcome To Video customers downloaded this video 369 times;

- d. File name “americanDad.mkv” with the video tag description “American dad all in one (toddler)” depicted an infant, approximately six months old. An adult male inserted his penis inside the mouth and anus of the infant. Welcome To Video customers downloaded this video 113 times;
- e. File name “中國他媽的男孩.mkv” with the video tag description “boy blow” depicted a male child, approximately ten years old. An adult male inserted his penis into the child’s mouth and anus while in a shower. Welcome To Video customers downloaded this video three times; and
- f. File name “cum in 8yo.mpg” with the video tag description “she whant [sic] sleep” depicted a female child, approximately eight years old. An adult male inserted his penis into the child’s anus. Welcome To Video customers downloaded this video 69 times.

Object of the Conspiracy

38. Numerous co-conspirators conspired with the defendant to upload child pornography videos files to Welcome To Video. The co-conspirators entered into this agreement to benefit:

- a. the defendant, who obtained illicit income as co-conspirators uploaded more videos files to Welcome To Video, which other customers then paid to access; and
- b. the co-conspirator uploaders, who derived points from the uploads, which they could redeem to download new video files from Welcome To Video.

Co-Conspirator Uploaders

39. Between on or about June 19, 2016, and or about January 16, 2017, co-conspirator “Zhch6z” uploaded over 100 videos to Welcome To Video. For example:

- a. On or about January 16, 2017, co-conspirator “Zhch6z” uploaded a video file entitled “Samantha Bathroom Facial.Flv” with the tag description “1958 Dr. Double X files from the producer of KansasKitty” to Welcome To Video. The video began by displaying the message “Samantha,” “5 Years Old,” and “Bathroom Facial,” after which a nude female child approximately five years old appeared. The female child was on her knees in a bathroom while an adult male masturbated and ejaculated on her face. Welcome To Video customers downloaded this video six times; and
- b. Included in the videos uploaded by co-conspirator “Zhch6z” were a series of videos of his approximately nine-year-old step-daughter engaged in sexually explicit conduct. For example, on or about October 19, 2016, “Zhch6z” uploaded a video file entitled “1797-1801 Thomas Jefferson.flv” with the tag description “KansasKitty” to Welcome To Video. The video depicted his approximately nine-year-old step-daughter nude, bent over, and with her buttocks spread apart so that her anus was visible while she inserted a dildo into her mouth. His step-daughter then inserted the dildo into her vagina. This video was downloaded by Welcome To Video customers ten times.

40. Between on or about May 2, 2016, and on or about May 11, 2016, co-conspirator

“dirtylad2k16” uploaded four videos to Welcome To Video. For example: On or about May 3, 2016, co-conspirator “dirtylad2k16” uploaded a video file entitled “VID-20160405-WA0007.mp4” with tag description “boy man rape fuck suck” to Welcome To Video. The video depicted a male toddler between the ages of one and two years old. After an adult male touched the male toddler’s penis, the adult male inserted his penis into the male toddler’s anus. Welcome To Video customers downloaded this video 13 times.

The Welcome To Video Server Was Located at Defendant’s Residence

41. On or about September 1, 2017, law enforcement reviewed the source code of Welcome To Video’s homepage, which could be viewed by right-clicking on the website and selecting “View Page Source.”

42. In reviewing the source code, law enforcement discovered that Welcome To Video failed to conceal one of its IP addresses, 121.185.153.64.

43. On or about October 24, 2017, law enforcement again observed that the Welcome To Video homepage failed to conceal another one of its IP addresses, 121.185.153.45.

44. These two IP addresses resolved to a telecommunications provider in South Korea and were registered to an account serviced at the defendant’s residence.

45. On or about March 5, 2018, a search of the defendant’s residence revealed the server for Welcome To Video located inside of his bedroom and actively operating.

The Defendant Was the Administrator of Welcome To Video

46. On or about September 28, 2017, an undercover agent in Washington, D.C. sent 0.03 BTC, worth at that time approximately \$124.72, to a BTC address that was provided by Welcome To Video. On or about September 30, 2017, the defendant then transferred these funds

to one of his BTC addresses ("Defendant's BTC Address 1").

47. On or about February 23, 2018, an undercover agent sent 0.03 BTC, worth at that time approximately \$287.79, to a BTC address that was provided by Welcome To Video. On or about February 24, 2018, the defendant then transferred these funds to Defendant's BTC Address 1.

48. On or about February 23, 2018, an undercover agent sent another 0.03 BTC to a another BTC address that was provided by Welcome To Video. On or about February 24, 2018, the defendant then transferred these funds to Defendant's BTC Address 1.

49. Defendant's BTC Address 1 was stored in an account ending in 209A at BTC Exchange 1. The signature card at BTC Exchange 1 revealed that this wallet was in the name of the defendant, and listed his cell phone number and his email account ("Defendant's Email Account 1").

50. On or about December 19, 2016, BTC Exchange 1 emailed Defendant's Email Account 1 a receipt for a BTC transaction involving the account ending in 209A cashing out BTC to a bank account ending in 0477.

51. The bank account ending in 0477 was held in the name of the defendant.

52. The defendant controlled at least four email accounts, all of which he repeatedly accessed from the IP address of 121.185.153.64, which was the IP address associated with Welcome To Video.

53. Beginning in at least July 2015, the defendant's Internet browsing and search history revealed multiple searches for, and visits to, Welcome To Video.

54. The defendant's Internet browsing and search history also revealed multiple

searches relating to child pornography, BTC, and computer coding.

User 123412 Was The Defendant, i.e., The Administrator

55. User “123412” was one of the defendant’s user names on Welcome To Video.

56. On or about November 17, 2015, the defendant emailed a file titled “1360201857305.mp4.” The defendant uploaded this same video, with the same title (“1360201857305.mp4”), to Welcome To Video via his user name “123412.”

57. The defendant uploaded videos to Welcome To Video via his user name “123412” with the description “Admin Upload.”

58. The coding of Welcome To Video allowed user “123412” to have unlimited download access to all videos on Welcome To Video.

59. The defendant uploaded approximately 779 video files to Welcome To Video via his user name “123412,” all of which occurred on or about June 15, 2015.

60. One of these video files was entitled “mrvine_c0092_fwrfw.mp4,” which depicted a pre-pubescent girl digitally penetrating her vagina.

COUNT ONE

61. Paragraphs 1 through 60 are incorporated here.

62. Beginning in or about June 2015, the exact date being unknown to the Grand Jury, and continuing through on or about March 5, 2018, within the District of Columbia and elsewhere, the defendant, Jong Woo Son, did knowingly conspire with “Zhch6z,” “dirtylad2k16,” and others known and unknown to the Grand Jury, to knowingly make, print, and publish, and cause to be made, printed, and published, a notice and advertisement, that is, a posting on Welcome To Video, seeking and offering to receive, exchange, buy, display, distribute, any visual depiction, the

production of which involved the use of a minor engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2)(A), and such visual depiction was of such conduct, knowing and having reason to know that such notice and advertisement would be transported using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, and such notice and advertisement was transported using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce by any means, including by computer, via the Internet.

(Conspiracy to Advertise Child Pornography, in violation of Title 18, United States Code, Section 2251(d) and (e)).

COUNT TWO

63. Paragraphs 1 through 60 are incorporated here.

64. Beginning in or about June 2015, the exact date being unknown to the Grand Jury, and continuing through on or about March 5, 2018, within the District of Columbia and elsewhere, the defendant, Jong Woo Son, did knowingly make, print and publish and cause to be made, printed and published, a notice and advertisement, that is, Welcome To Video, seeking and offering to receive, exchange, buy, display, distribute, any visual depiction, the production of which involved the use of a minor engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2)(A), and such visual depiction was of such conduct, knowing and having reason to know that such notice and advertisement would be transported using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce by any means, including by computer, and such notice and advertisement

was transported using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, via the Internet.

(Advertising Child Pornography, in violation of Title 18, United States Code, Section 2251(d)).

COUNT THREE

65. Paragraphs 1 through 60 are incorporated here.

66. Beginning in or about June 2015, the exact date being unknown to the Grand Jury, and continuing through on or about March 5, 2018, within the District of Columbia and elsewhere, the defendant, Jong Woo Son, while outside the United States, that is, South Korea, did knowingly transport, distribute, and sell any visual depiction of a minor engaging in sexually explicit conduct, that is, the video files on Welcome To Video, the production of which visual depiction involved the use of a minor engaging in sexually explicit conduct, intending that such visual depiction would be imported into the United States.

(Production of Sexually Explicit Depictions of a Minor for Importation Into The United States, in violation of Title 18, United States Code, Section 2260(b))

COUNT FOUR

67. Paragraphs 1 through 60 are incorporated here.

68. Beginning in or about June 2015, the exact date being unknown to the Grand Jury, and continuing through on or about March 5, 2018, within the District of Columbia and elsewhere, the defendant, Jong Woo Son, did knowingly conspire with “Zhch6z,” “dirtylad2k16,” and others known and unknown to the Grand Jury, to knowingly distribute any visual depiction using any means and facility of interstate and foreign commerce, including by

computer, where the visual depiction involved the use of a minor engaging in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2)(A), and such visual depiction is of such conduct.

(Conspiracy to Distribute Child Pornography, in violation of Title 18, United States Code, Section 2252(a)(2) and (b)(1)).

COUNT FIVE

69. Paragraphs 1 through 60 are incorporated here.

70. On or about September 28, 2017, within the District of Columbia and elsewhere, the defendant, Jong Woo Son, did knowingly distribute any visual depiction, to include video files (a) “mrvine_c0092_fwrfw.mp4,” (b) “Samantha Bathroom Facial.vlf,” and (c) “2 (2).avi,” using any means and facility of interstate and foreign commerce, including by computer, where the visual depiction involved the use of a minor engaging in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2)(A), and such visual depiction is of such conduct.

(Distribution of Child Pornography, in violation of Title 18, United States Code, Section 2252(a)(2))

COUNT SIX

71. Paragraphs 1 through 60 are incorporated here.

72. On or about February 22, 2018, within the District of Columbia and elsewhere, the defendant, Jong Woo Son, did knowingly distribute any visual depiction, to include video files (a) “[pthc] 10y Tara Blowjob + Anal Riding Fuck (05min).avi,” (b) a video with a foreign language title and an English description stating “boy blow,” and (c) “cum in 8yo.mpg,” using any means and facility of interstate and foreign commerce, including by computer, where the

visual depiction involved the use of a minor engaging in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2)(A), and such visual depiction is of such conduct.

(Distribution of Child Pornography, in violation of Title 18, United States Code, Section 2252(a)(2))

COUNTS SEVEN THROUGH NINE

73. Paragraphs 1 through 60 are incorporated here.

74. On or about the dates described, within the District of Columbia and elsewhere, the defendant, Jong Woo Son, caused the transmission and transfer, of a monetary instrument and funds, in the amounts described below, from a place in the United States, that is, Washington, D.C., to or through a place outside the United States, that is South Korea, with the intent to promote the carrying on of specified unlawful activity, that is, section 2252A (relating to child pornography) where the child pornography contains a visual depiction of an actual minor engaging in sexually explicit conduct, and section 2260 (production of certain child pornography for importation into the United States).

<u>Count</u>	<u>On or about Date of Transfer</u>	<u>Amount of Bitcoin</u>
Seven	October 30, 2015	.13
Eight	October 24, 2016	.1305
Nine	September 28, 2017	.03

(Laundering of Monetary Instruments, in violation of Title 18, United States Code, Section 1956(a)(2)(A))

FORFEITURE ALLEGATION

1. Upon conviction of any the offenses alleged in Counts One through Six, the defendant shall forfeit to the United States any visual depiction described in Title 18, United States Code, Sections 2251, 2252, or 2260, or any book, magazine, periodical, film, videotape, or other matter which contains any such visual depiction, which was produced, transported, mailed, shipped or received in violation of Title 18, United States Code, Chapter 110; any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from this offense; and any property, real or personal, used or intended to be used to commit or to promote the commission of this offense or any property traceable to such property, pursuant to Title 18, United States Code, Section 2253(a). The United States will also seek a forfeiture money judgment against the defendant equal to the value of any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from these offenses; and any property, real or personal, used or intended to be used to commit or to promote the commission of these offenses or any property traceable to such property.

2. Upon conviction of the offenses alleged in Counts Seven through Nine of this Indictment, the defendant shall forfeit to the United States any property, real or personal, involved in these offenses, or any property traceable to such property pursuant to Title 18, United States Code, Section 982(a)(1). The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, involved in these offenses, and any property traceable to such property.

3. The specific property subject to forfeiture includes four hard drives seized on March 5, 2018 from the defendant's residence.

4. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

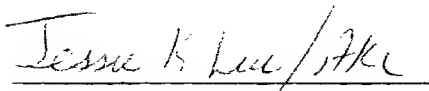
- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be divided without difficulty;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(**Criminal Forfeiture**, pursuant to Title 18, United States Code, Section 2253(a), Title 18, United States Code, Section 982(a) and Title 21, United States Code, Section 853(p)).

A TRUE BILL

FOREPERSON



Attorney of the United States
And for the District of Columbia